**Statement of Assistant Secretary for Infrastructure Protection**
**Robert B. Stephan**
**U.S. Department of Homeland Security**
**Before the Economic Security, Infrastructure Protection, and Cyber Security Subcommittee**
**of the House Homeland Security Committee**
**October 20th, 2005**

## Introduction

Good morning, Mr. Chairman, Ranking Member Sanchez and distinguished Members of this Subcommittee. I appreciate the opportunity to speak with you.

The Department of Homeland Security is committed to working with our partners in State, local and tribal governments and the private sector in reducing the overall level of risk of terrorist attacks against our national critical infrastructure. By reducing risk, we mean examining the consequences of a potential attack; examining the vulnerability of critical sites and facilities to various modes of attack; and examining the potential threat — that is, the intent of terrorists to attack in a given place and their likelihood of success.

In analyzing risk, it becomes clear that certain means of attack against certain types of targets are easier for terrorists to accomplish and difficult for us to protect against. The July 7 and 21 attacks on the London mass transit system in 2005, as well as the March 2004 attack in Madrid, underscore the inherent vulnerability of open-access systems.

Recognizing that despite our best efforts, we cannot always protect everyone against all dangers, this risk-based approach allows us to make better judgments about where we target resources and prioritize our protection efforts.

In working to reduce risk and protect critical infrastructure, DHS has three principal objectives:

- Provide resources and training to State and local governments and law enforcement for security enhancements;
- Provide information to both public and private sectors on the threat environment, tactics and techniques of terrorists, common vulnerabilities and suggested protective measures; and
- Create information-sharing mechanisms that enable DHS stakeholders to share best practices and the unique aspects of their assets to improve situational awareness during a crisis or when faced with a specific threat.

## The National Infrastructure Protection Plan

These objectives are being realized through the implementation of the National Infrastructure Protection Plan (NIPP). Directed by Homeland Security Presidential Directive 7 (HSPD-7), the NIPP is a unified national plan for the consolidation of critical infrastructure protection (CIP) activities. The NIPP is a collaborative effort between the private sector, State, local, territorial and tribal entities and all relevant departments and agencies of the Federal government.

The cornerstone of the NIPP is a risk management framework that combines threat, vulnerability, and consequence information to produce a comprehensive, systematic, and informed assessment of national or sector risk that drives our risk reduction efforts in the critical infrastructure/key resources (CI/KR) sectors. This framework applies to the general threat environment as well as specific threats or incident situations.

**NIPP Risk Management Framework**

**Set Security Goals.** Achieving a secure, protected, and resilient infrastructure requires a common set of national and sector-specific security goals that address those aspects of risk that can be affected and collectively represent an acceptable security posture. Therefore, sector security goals will be determined through a collaborative effort of government agencies and the private sector. Establishing sector security goals is the nexus of the NIPP planning process that will drive the public/private partnership. Nationally, the overarching security goal of reducing risk begins with an enhanced state of CI/KR security, a state which is best achieved through the implementation of focused risk reduction and protective strategies across the critical sectors.

**Identify Assets.** Once security goals are set, the next step in the framework is to develop and maintain an inventory of the Nation's assets. First, asset information is collected and catalogued in the National Asset Database (NADB), which is the central Federal repository for national infrastructure-related information. Second, after an asset is identified and basic information on it is collected, DHS employs an initial screening methodology to determine whether or not it is of national consequence. Finally, priority is given to applying federal resources to those assets that, if attacked, could have a nationally significant effect

**Assess Risk.** If an asset is determined to be of national consequence, it is then subjected to a risk analysis. As mentioned before, risk is determined through a combined assessment of:

- Consequence — estimates of the damage a successful attack would cause;
- Threat — estimates of the likelihood that a particular target or type of target will be selected for attack; and
- Vulnerability — assess which elements of infrastructure are most susceptible to attack and how attacks against these elements would be most likely carried out.

One of the Department's principal risk-assessment tools is RAMCAP (Risk Assessment Methodology for Critical Asset Protection). RAMCAP is being developed by DHS in collaboration with other federal agencies and the private sector as a sector-specific consequence, vulnerability, and risk methodology. RAMCAP enables an assessment and comparison of risk of critical infrastructure assets both across and within CI/KR sectors, thereby enabling the prioritization of protective efforts and effective use of available resources.

**Prioritize.** It is impossible, nor do we attempt, to protect all CI/KR equally across the entire United States. We assess the potential consequences of an attack, threats, and vulnerabilities for CI/KR sectors, as well as individual assets within those sectors and prioritize our efforts based upon the severity and mass effect of potential consequence. Conducting risk analysis provides us with the

information needed to make such determinations, as well as provides the department a basis upon which to make longer-term resource decisions including strategic protective programs and planning for response and other contingency situations.

**Implement Protective Programs.** The widely dispersed nature of critical infrastructure demands equally dispersed ownership and execution of protection programs. It requires centralized leadership which in turn drives consistent implementation and ensures the greatest cost-benefit through addressing the greatest risks. DHS leads the Federal government's critical infrastructure protection effort, and works in collaboration with State and local governments, the private sector, and our international partners to protect against potential terrorist attacks through reducing our vulnerabilities and enhancing our response capabilities to potential terrorist attacks. Some of the key DHS programs include:

- **Vulnerability Identification Self-Assessment Tool** — An important initiative designed to increase the capabilities of private sector owners and operators to enhance their own security is the DHS Vulnerability Identification Self-Assessment Tool (DHS-VISAT). This is a voluntary, on-line assessment tool that was originally developed to help transportation asset owner/operators enhance security. The goal of this program is to raise the level of security awareness in public assembly facilities across the nation and establish a common "baseline" of security awareness from which these facilities can build their protection plans. To date, it has been adapted for use by stadium and arena managers and access has been provided to over 300 stadiums and 400 arenas. Currently this tool is being modified for use by other commercial venues including convention and performing arts centers. In addition, we have engaged in piloting efforts with the States of Texas, Virginia, and California to adapt the tool to support security awareness in K-12 schools.

- **Target Awareness Training** — The Target Awareness Training (TAT) program provides baseline prevention and awareness training to first level supervisors and security personnel and is supported by VISAT. The primary objectives of TAT are to increase the ability to deter and detect potential attacks and to increase the reporting of suspicious activity and suspect items. The courses focus on law enforcement and security staff working in shopping malls and centers, places of worship, educational institutions, hotels, and sports complexes. Over 2,500 law enforcement and private sector personnel have participated in 128 TAT Courses since September 2003. We also provide a Surveillance Detection Course, Surface Transportation Antiterrorism Program, and an Improvised Explosive Devices/Weapons of Mass Destruction (IED/WMD) Electronics course.

- **Bomb Prevention** — Bombing is a preferred tactic for terrorists seeking relatively uncomplicated, inexpensive means for harming large numbers of people and inflicting maximum damage on critical infrastructure. The threat that IEDs and other types of explosive weapons pose are of great concern given the relative technological ease with which such an attack could be planned and executed. Central to preventing bombing attacks are:

    - the need for new critical thinking and analysis regarding the nature and scope of preventing an attack;

- innovation in detection, deterrence, and improving system robustness in the face of an adaptable enemy;
- the importance of increased stakeholder participation and cooperation;
- the need for more robust information sharing and collaboration measures; and
- meaningful dialogue between State and local jurisdictions and the Federal government to identify and fill operational capability gaps related to training, equipment, technology and resources

We will continue to assist state and local entities in identifying gaps in protective capacity and obtaining required resources. Under Homeland Security Presidential Directive-8 and the National Preparedness Goal, the Department is identifying bomb prevention capabilities at every level of the government and identifying gaps in this capability. We are taking steps to address any gaps that exist by developing a focused and unified national bombing prevention effort through such groups as the Interagency Governance Board and the IED Task Force. DHS is also developing enhanced knowledge management systems that foster information sharing and collaboration between Federal, State, and local entities involved in bombing prevention, and among various and disparate law enforcement jurisdictions.

**Information Sharing**

One of the principal goals of the Federal-State-local-private sector partnership is to provide the necessary framework and support to enable coordination and information sharing within each CI sector, across all CI sectors, and between all levels of the government and private sector in order to achieve the execution of a full spectrum of prudent and responsible protective actions.

- **Sector Partnership Model** — Under the NIPP framework, DHS is helping to create private sector-led Sector Coordinating Councils (SCCs) for each of the 17 critical infrastructure sectors. These councils will serve as a mechanism for identifying risk and protection issues within their specific sector and addressing the range of infrastructure protection activities. For example, the "Commercial Facilities" sector coordinating council encompasses open-access facilities that, if attacked, could cause significant casualties and economic damage. Accordingly, membership in the Commercial Facilities SCC includes all major sports leagues, International Council of Shopping Centers, Marriott, Warner Brothers, Disney, the Real Estate Roundtable, the Self Storage Association, the International Association of Assembly Managers, and others.

  Both the SCCs, and their government counterparts, Government Coordinating Councils (GCCs) will increase inter-agency coordination and information sharing on critical infrastructure protection activities. ~~Like the SCC,~~ The GCC coordinates strategies, activities, policy, and communication across organizations within each sector. Unlike the SCC, it does so through the Federal government. The SCC and GCC work together to create a coordinated national mechanism for infrastructure protection in their sector. Members of the Commercial Facilities GCC include the US Secret Service, the Federal Protective Service, the Environmental Protection Agency, the General Services Administration, and the Departments of Commerce, Justice, Interior, and Education.

- **Homeland Security Information Network** — DHS is developing a networked approach to information-sharing that enables rapid information dissemination to decentralized decision makers across the nation. The key objectives of this approach are to enable multi-directional information sharing between and across government and industry; provide all CI/KR sector owners and operators with a robust communications framework, tailored to the specific information sharing requirements of each sector; and provide a comprehensive threat landscape to all security partners, including general and specific threats, incidents and events, impact assessments, and best practices.

  At the core of this networked approach is a series of sophisticated, secure tools and support mechanisms, collectively referred to as the Homeland Security Information Network (HSIN), which provides a national communications platform that enables the flow of near real-time information among governmental entities at all levels (i.e., Federal, state, territorial, local, and tribal), private sector organizations, and international security partners.

- **National Infrastructure Coordinating Center** — The National Infrastructure Coordinating Center (NICC) is a 24x7 watch operation center that maintains operational and situational awareness of the Nation's CI/KR sectors. The fully operational NICC provides a centralized mechanism for gathering information and a process for sharing and coordinating information between and among government, SCCs, GCCs, and other industry partners. The NICC receives incident reports from specific sectors in accordance with pre-established information-sharing standard operating procedures. When required, the NICC also disseminates a wide range of products containing warning, threat, and critical infrastructure protection (CIP) information to the private sector and government entities. The NICC is also responsible for receiving situational and operational information from the private sector and disseminating that information throughout the Homeland Security Operations Center (HSOC), other government operation centers, and industry partners as applicable.
- **Information Sharing and Analysis Center** — The private sector has established a number of information-sharing mechanisms that contribute to the protection of their assets. One such mechanism is the Information Sharing and Analysis Center (ISAC). While the SCCs ultimately define the unique information-sharing requirements for each sector, ISACs and other existing mechanisms provide an array of options and capabilities for some infrastructure owners and operators.

  ISACs, while varying greatly in composition, scope, and capabilities, offer a viable information-sharing mechanism. Some ISACs, for example, maintain 24x7 watch centers and provide various levels of sector-specific alerting and analysis. In this regard, the Surface Transportation and Public Transportation ISAC collects, analyzes, and distributes critical cyber and physical security and threat information from government and numerous other sources on a 24/7 basis. Other ISACs maintain a watch center that is staffed during traditional business hours, with the ability to contact analysts via telephone or pager during periods of increased activity. Still others operate primarily through Websites, allowing members to access sector-related alerts, warnings, and incident information. Regardless of the variance in breadth and depth, however, ISACs are capable of disseminating DHS-issued threat information.

- **International Information Sharing** — We have made significant progress in cooperation with our international partners in the war on terror to share best practices and intelligence. This is especially true in the area of bombing prevention. The United Kingdom and Israel have years of experience in bombing prevention. DHS has and will continue to work closely with Scotland Yard and the Israeli Defense Force and police in order to learn better methods of bombing detection and prevention.

  Additionally, we are part of the Department of Defense's effort in the Joint Improvised Explosive Device-Defeat Task Force, an interagency, international effort with Israeli, Australian, Canadian, and British participation. The task force will establish an open-door program of international partners who will work to develop and exchange detection and prevention technologies.

**Reacting to Crisis**

In the immediate aftermath of the July 7, 2005, attacks in London, DHS stood up the Interagency Incident Management Group (IIMG) to serve as the national headquarters-level multi-agency coordination entity for incident management. Secretary Chertoff then recommended to the President that the Homeland Security Advisory System (HSAS) move from YELLOW to ORANGE for the Mass Transit Sector. In response, the Office of Infrastructure Protection, in partnership with TSA, coordinated outreach with public and private sector owners and operators in the Mass Transit Sector to provide them with an overview of the latest threat intelligence, to explain the implications of a move to ORANGE, and to provide them an opportunity discuss those implications.

We worked with our Federal partners to enhance security at our Nation's largest mass transit systems and made Urban Area Security Initiative (UASI) funding available for overtime to State and local law enforcement for activities related to increased mass transit security. Our intelligence and analytical units produced Joint Advisories and Information Bulletins with the FBI that detailed what we knew about the terrorists target selection, attack methodology, implications, and suggested protective measures that mass transit operators could implement. Following the attacks, personnel from the Office of Infrastructure Protection and TSA conducted analysis of mass transit systems, starting in large cities such as the New York and New Jersey systems. Inspectors from the Federal Railroad Administration conducted inspections of passenger rail operations in the days immediately following the July 7 attacks. Throughout this process, DHS effectively executed its mission as a coordinator of national critical infrastructure protection efforts, and served as the focal point for information sharing both within the Federal government and between the public and private sectors.

**Conclusion**

DHS is dedicated to working with infrastructure stakeholders across the country to increase the security of our Nation's critical infrastructure sectors using a risk-based approach. The places and events where our fellow citizens are most vulnerable are a key priority. With your support and that of the American people, we will succeed. Thank you.